主要内容

五、Web安全（续）
- ❖针对服务器的攻击
- ❖针对客户端的攻击

六、网络协议的脆弱性
- ❖各层协议的安全性
  - ➢ARP欺骗，IP欺骗，TCP会话劫持
- ❖拒绝服务攻击DOS
  - ➢ ICMP攻击
  - ➢ SYN洪泛攻击

Web安全

（续）

Web应用程序安全

◆漏洞攻击者利用不安全的Web应用程序来危害整个服务器，或破坏一个网站。

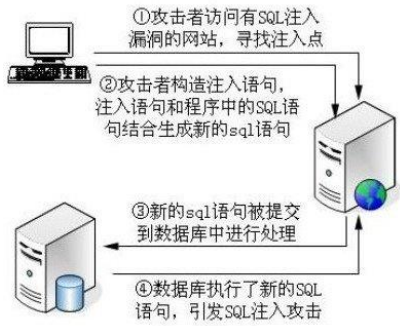
◆主要WEB 漏洞（Vulnerabilities）
- ❖SQL 注入攻击（SQL Injection）
- ❖跨站域请求伪造(CSRF – Cross-site request forgery)
- ❖跨站脚本攻击(XSS – Cross-site scripting)

SQL 注入攻击

◆产生原因
- ❖SQL注入往往是在编写包含用户输入的动态数据库查询时产生的
- ❖程序员在Web开发时，没有过滤特殊字符，绑定变量，导致攻击者可以通过SQL灵活多变的语法，构造特殊语句，达成目的，或者通过系统报错，返回对自己有用的信息。
  - ➢浏览器将错误（恶意）输入发送给服务器
  - ➢缺乏必要的输入合法性检查导致错误的 SQL 查询

◆危害
- ❖整个数据库的信息都能被读取或篡改
- ❖获得更多的包括管理员的权限

SQL 注入攻击过程



例子

- 填好正确的用户名(tarena)和密码(admin)后，点击提交
  - 根据我们提交的用户名和密码被合成到SQL查询语句：
  - select * from users where username='tarena' and password=md5('admin')
- 对于有SQL注入漏洞的网站来说，只要构造个特殊的“字符串”，照样能够成功登录
  - 例如，在用户名输入框中输入:' or 1=1#,密码随便输入，这时候的合成后的SQL查询语句为：
  - select * from users where username='' or 1=1#' and password=md5('')
  - “#”在mysql中是注释符，等价于：

    select * from users where username='' or 1=1

因为1=1永远都是成立的，即where子句总是为真，将该sql进一步简化之后，等价如下select语句：

select * from users

危害

- 数据表中的数据外泄，例如个人机密数据，账户数据，密码等。
- 数据结构被黑客探知，得以做进一步攻击（例如SELECT * FROM sys.tables）。
- 数据库服务器被攻击，系统管理员账户被窜改（例如ALTER LOGIN sa WITH PASSWORD='xxxxxx'）。
- 获取系统较高权限后，有可能得以在网页加入恶意链接以及XSS
- 经由数据库服务器提供的操作系统支持，让黑客得以修改或控制操作系统（例如xp_cmdshell “net stop iisadmin”可停止服务器的IIS服务）。
- 破坏硬盘数据，瘫痪全系统（例如xp_cmdshell “FORMAT C:”）。

防御SQL 注入攻击

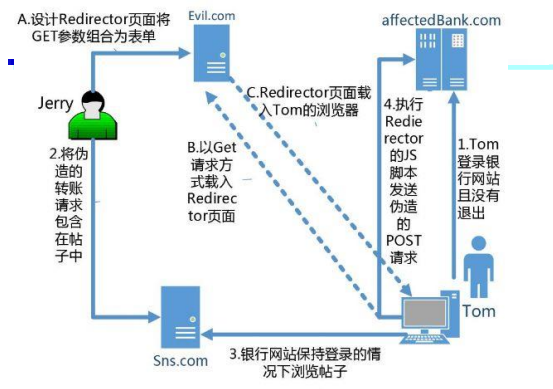
- 用户输入验证
  - 对用户的输入进行校验，可以通过正则表达式，或限制长度，对单引号和双"-"进行转换等。
  - 不要使用动态拼装SQL，可以使用参数化的SQL或者直接使用存储过程进行数据查询存取。
- 权限管理
  - 不要使用管理员权限的数据库连接，为每个应用使用单独的权限有限的数据库连接。
- 其他
  - 不要把机密信息按明文形式存放。
  - 应用的异常信息应该给出尽可能少的提示，最好使用自定义的错误信息对原始错误信息进行包装，把异常信息存放在独立的表中

跨站域请求伪造 CSRF

- CSRF(Cross Site Request Forgery)是一种依赖web浏览器的、被混淆过的代理人攻击（deputy attack）。
  - 该攻击可以在受害者毫不知情的情况下以受害者名义伪造请求发送给受攻击站点，从而在并未授权的情况下执行在权限保护之下的操作，有很大的危害性。
  - 产生原因：Web隐式身份认证机制

CSRF原理

- CS=Cross Site，跨站；RF=Request Forgery，请求伪造
- 原理
  - 用户C打开浏览器，访问受信任网站A，输入用户名和密码请求登录网站A;
  - 在用户信息通过验证后，网站A产生Cookie信息并返回给浏览器，此时用户登录网站A成功，可以正常发送请求到网站A;
  - 用户未退出网站A之前，在同一浏览器中，打开一个TAB页访问网站B;
  - 网站B接收到用户请求后，返回一些攻击性代码，并发出一个请求要求访问第三方站点A;
  - 浏览器在接收到这些攻击性代码后，根据网站B的请求，在用户不知情的情况下携带Cookie信息，向网站A发出请求。网站A并不知道该请求其实是由B发起的，所以会根据用户C的Cookie信息以C的权限处理该请求，导致来自网站B的恶意代码被执行。



重定向实现POST请求的CSRF

说明

- 攻击从用户的浏览器发起，通过共享cookie来伪造请求
- 可以伪造的请求，与网站A存在CSRF漏洞的页面有关
  - 例如，网站B可以通过GET方式和POST方式，伪造请求给网站A；但无法通过Ajax进行请求伪造，这是因为浏览器遵循的Ajax的跨域限制。
- CSRF危害更多是针对可以进行业务动作（增删改）的页面，通过伪造请求欺骗站点进行业务办理。
- 对于查询页面存在CSRF漏洞，由于浏览器跨域限制，即使请求返回数据，网站B的页面是无法对数据进行分析或处理，因此查询页面的CSRF危害会小很多，或者没有危害。

防御CSRF漏洞

- 服务端的防御：在客户端页面增加伪随机数
  - 验证HTTP Referer字段（该HTTP请求的来源地址）
  - 在请求地址中添加令牌token并验证。在请求中放入攻击者所不能伪造的信息，并且该信息不存在于Cookie之中
  - 在HTTP头中自定义属性并验证
- 用户端的防御
  - 当用户关闭页面时要及时清除认证cookie
  - 尽量少用或不要用request()类变量，增加CSRF攻击的难度 。
- 安全设备的防御

跨站脚本攻击XSS

- XSS (Cross Site Script)，跨站脚本攻击
  - 恶意攻击者往Web页面里插入恶意脚本代码，而程序对于用户输入内容未过滤，当用户浏览该页之时，嵌入其中Web里面的脚本代码会被执行，从而达到恶意攻击用户的特殊目的。
- 危害
  - 窃取cookie、放蠕虫、网站钓鱼
- 分类
  - 存储型XSS、反射型XSS、DOM型XSS
- XSS几乎每个网站都存在
  - google、baidu、360等

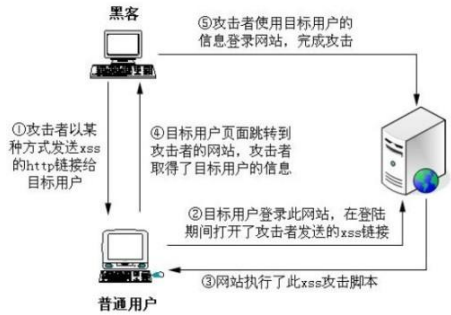
三种类型 XSS

- 反射型Reflected XSS
  - 主要依靠站点服务端返回脚本，在客户端触发执行从而发起Web攻击
- 存储型Stored XSS
  - 是通过发表带有恶意跨域脚本的帖子/文章，从而把恶意脚本存储在服务器，每个访问该页面的人就会触发执行。
- DOM型或本地 XSS
  - 通常提供免费wifi的网关会往你访问的任何页面插入一段脚本或者是直接返回一个钓鱼页面，从而植入恶意脚本。这种直接存在于页面，无须经过服务器返回就是基于本地的XSS攻击。（流量劫持）

跨站脚本攻击XSS攻击过程

- 攻击者以某种方式发送xss的http链接给目标用户
- 目标用户登录此网站，在登陆期间打开了攻击者发送的xss链接
- 网站执行了此xss攻击脚本
- 目标用户页面跳转到攻击者的网站，攻击者取得了目标用户的信息
- 攻击者使用目标用户的信息登录网站，完成攻击

跨站脚本攻击XSS攻击过程



防御XSS攻击

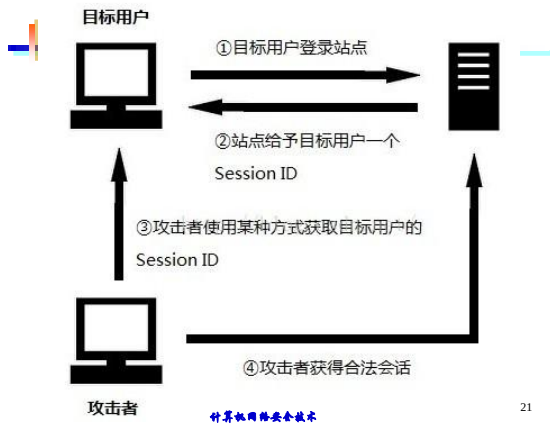
- 前端在显示服务端数据时候，考虑过滤转义标签内容、属性值、恶意脚本
- 后端接收请求时，验证是否为攻击请求
- 服务端也要进行过滤，因为前端的校验可以被绕过。
- 使用HTTPS
- HTML5 制定了一套浏览器XSS 解决方案 CSP（Content Security Policy）大多主流浏览器实现了这个标准。
  - 更大的攻击面，HTML5带来来更多的标签和更多的属性，XSS发生的可能性更大。
  - 更大的危害，HTML5更多的资源可以被XSS利用，包括可以利用浏览器的一切权限，比如本地存储，GEO，WebSocket，Webworker。

针对Web客户端的攻击（1）

- **什么是会话?**
  - 服务器端是通过来自客户端的一个身份标识来认证用户，为了维持来自同一个用户的不同请求之间的状态， 客户端必须要给服务器端发送一个唯一的身份标识符(Session ID)
- 攻击者获取一个有效的session ID
  - 预测：类似暴力破解，猜测出系统中使用的有效的session标识符，难度大
  - 会话劫持：取得一个合法的会话标识来伪装成合法用户
  - 会话固定：诱骗受害者使用攻击者指定的会话标识
- **会话劫持（session hijacking）**
  - 攻击者首先通过捕获合法用户的session, 然后冒充该用户来访问系统
  - 攻击者至少必须要获取到一个有效的session标识符，用于后续的身份认证

会话劫持

- 目标用户需要先登录站点；
- 登录成功后，该用户会得到站点提供的一个会话标识SessionID；
- **攻击者通过某种攻击手段捕获Session ID**；
- 攻击者通过捕获到的Session ID访问站点即可获得目标用户合法会话。



防御HTTP会话劫持

- 第一道防线
  - 防止数据包嗅探器（流量分析攻击）和TCP会话劫持
- 防止攻击者重建有效的服务器端会话令牌
  - 加密会话令牌
  - 使用随机数生成服务器端会话ID
- 防范重放攻击
  - 经常改变会话令牌，限制令牌的有效期
  - 将会话令牌与客户端IP地址相关联

针对Web客户端的攻击（2）

- 网络钓鱼（phishing）
  - 企图利用人们对著名品牌、网站和机构的信任，通过网络进行诈骗活动的行为，都可以称为“网络钓鱼”。
  - 攻击者会伪装成信誉良好的实体或个人通过电子邮件或其他通信渠道，使用网络钓鱼电子邮件分发可执行各种功能的恶意链接或附件，从受害者中提取登录凭据或帐户信息；或者自动下载恶意软件，让受害者使用恶意软件感染自己的计算机。
- 钓鱼网站，即假网站
  - 传统意义上指的是利用伪造银行网站的方式，窃取用户银行帐号的行为。
  - 例如，一个正确的网站www.qqpet.qq.com，而钓鱼网站可能变成了www.qqqet.qq.com

网络协议的脆弱性

漏洞

- 漏洞，又称脆弱性(vulnerability)，是计算机系统在硬件、软件、协议的具体实现和系统安全策略上存在缺陷和不足，从而可以使攻击者能够在未授权的情况下访问或破坏系统
- 漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用的漏洞的一种安全检测（渗透攻击）行为。

漏洞的分类

- 从脆弱性来源划分
  - 系统配置不当导致的脆弱性
  - 各种系统软件、应用软件存在脆弱性
  - 网络或系统的某些功能自身存在安全隐患
  - 操作系统本身存在安全隐患

网络攻击的角度

- 非法获取系统操作权限
- 执行任意代码
- 非法读写系统文件
- 拒绝服务
- 口令获取
- 服务信息泄漏
- 伪造信息欺骗
- 设置后门

漏洞管理

- 漏洞分级
  - 根据对系统造成的潜在威胁以及被利用的可能性可将各种安全漏洞进行分级
  - 分为高、中、低3级
- 漏洞库
  - 把所有系统安全漏洞及其相关信息存储到数据库中，方便计算机用户更详细地了解系统安全漏洞，方便用户检索自己的系统会存在哪些漏洞，可能对系统安全造成什么危害以及如何补救等等

国内主要公布漏洞的站点

- 中国国家信息安全漏洞共享平台(由CNCERT维护): http://www.cnvd.org.cn
- 国家信息安全漏洞库(由中国信息安全评测中心维护)：http://www.cnnvd.org.cn/
- 绿盟科技-安全漏洞：http://www.nsfocus.net/index.php?act=sec_bug
- 中国教育和科研计算机网紧急响应组（www.ccert.edu.cn）
- 中国国家工控系统行业漏洞：http://ics.cnvd.org.cn/
- …

国外常用漏洞库

- 赛门铁克的漏洞库 https://www.securityfocus.com/
- 美国国家信息安全漏洞库 https://nvd.nist.gov/
- 全球信息安全漏洞指纹库与文件检测服务 http://cvescan.com
- 美国著名安全公司Offensive Security的漏洞库 https://www.exploit-db.com/
- CVE(美国国土安全资助的MITRE公司负责维护) https://cve.mitre.org/
- 美国国家工控系统行业漏洞库 https://ics-cert.us-cert.gov/advisories

网络协议的脆弱性

- ARP欺骗
- IP欺骗
- TCP会话劫持

对局域网的攻击：LAN

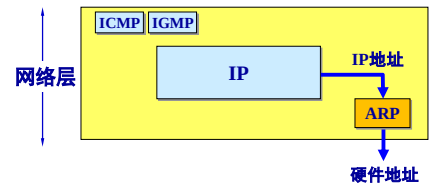
- 例如：攻击者控制了局域网中的某台PC机
- 攻击者的行为
  - 安装数据包嗅探软件
  - 获取密码，甚至根密码
  - 接管相应的账号。
- 防御方法：阻止密码嗅探攻击
  - 使用挑战-应答密码生成器
  - Kerberos
  - ssh协议(保证LAN上不会有明文密码传送)

对局域网的攻击：WLAN

- 欺骗访问点(非法AP，Rogue Access Point)
  - 公共区域中的WiFi热点，例如机场，但该访问点已被恶意部署。
  - 如果用户使用该接入点，黑客就可以嗅探用户输入的明文密码，或将用户导向到恶意站点。
  - 此外，欺骗访问点也可能是雇员为了自己方便而违反公司安全策略要求安装的设备
  - 也可以是错误配置(以至于不能对网络流量进行加密)的正式节点。

地址解析协议 ARP 的作用

- 已经知道了一个机器（主机或路由器）的IP地址，如何找出其相应的硬件地址？
- 地址解析协议 ARP 就是用来解决这样的问题的



ARP 协议的作用

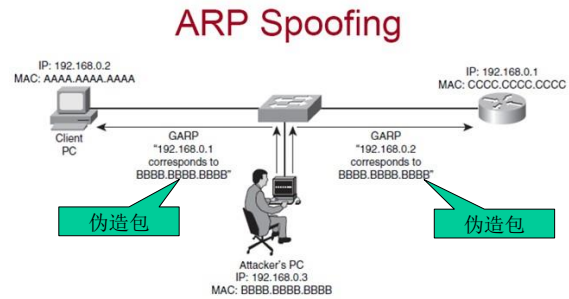
ARP 作用：从网络层使用的 IP 地址，解析出在数据链路层使用的硬件地址。

ARP欺骗攻击

- ARP攻击主要存在于局域网网络中
- 攻击方法：通过伪造IP地址和MAC地址实现ARP欺骗
  - 能够在网络中产生大量的ARP通信量使网络阻塞，
  - 持续不断的发出伪造的ARP响应包就能更改目标主机ARP缓存中的IP-MAC条目，造成网络中断或中间人攻击
- 局域网中若有一台计算机感染ARP木马，则感染该ARP木马的系统将会试图通过“ARP欺骗”手段截获所在网络内其它计算机的通信信息，并因此造成网内其它计算机的通信故障。

ARP欺骗攻击

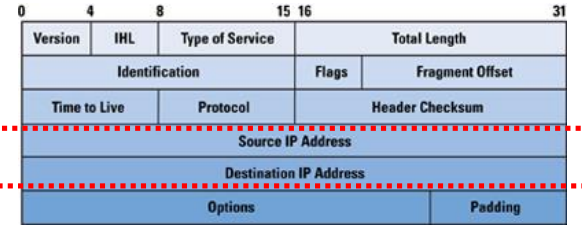
- **ARP欺骗攻击（ARP毒化，ARP缓存中毒）**
- **Gratuitous ARP（GARP）：主机使用自己的IP地址作为目标地址发送ARP请求**



IP欺骗

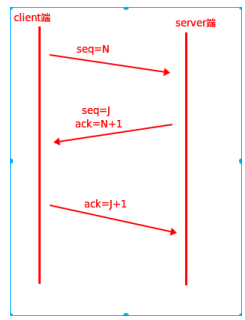
- IP spoofing (IP 欺骗)
  - 用伪造的源IP地址来发送 IP 数据包，例如，采用可信源的 IP 地址来尝试绕过防火墙
  - 这将使防火墙误以为来自入侵者的数据包是来自可信源端的
  - IP 欺骗也可以仅用于隐藏攻击的真实来源
- 能否收到响应包?
  - 由于入侵者伪装成他人出现，因此，如果发送响应，该响应将发往入侵者所伪造的地址，而非其真实地址。
- 结合其他中间人攻击
  - TCP劫持
  - 拒绝服务攻击

IP分组首部格式



TCP会话劫持

- TCP会话劫持（ TCP Session Hijack ）
  - TCP连接建立过程：**三次握手**
    - 序号Seq
    - 应答Ack
  - 为了生成一个伪造TCP数据包，攻击者需要获得特定TCP连接的当前识别信息
- 同一网段攻击
  - 数据包嗅探
  - 注入可能的序列号和命令
- 跨网段攻击
  - TCP序列预测：用数学方法猜测TCP连接的初始数值
  - 利用信任关系进行服务器攻击（ rlogin，rsh，rcmd ）



TCP报文段首部

拒绝服务攻击

拒绝服务攻击

- 拒绝服务器攻击的基本概念
- ICMP攻击（smurf攻击）
- SYN洪泛攻击
- 其他攻击方法

拒绝服务攻击DoS

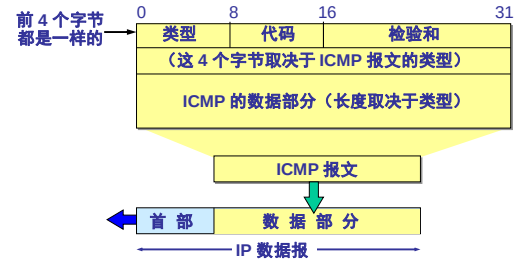
- Denial-of-Service， DoS
  - 它是以**瘫痪目标为目的**，而不是窃取数据，是典型的损人不利己的行为
  - 它**发起攻击比较容易**，很隐蔽
  - 它具有很大的**随意性**
- DoS是最难防御的攻击之一，只有全面防御才可能减少损害
- 如何防御?
  - 主机设置
  - 网络设备设置：防火墙，路由器
  - 安装专门的DoS识别和预防工具

ICMP攻击

网际控制报文协议 ICMP

- 为了提高 IP 数据报交付成功的机会，在网际层使用了网际控制报文协议 ICMP (Internet Control Message Protocol)。
- ICMP 允许主机或路由器报告差错情况和提供有关异常情况的报告。
- ICMP 协议的封装
  - 是IP 层的协议
  - 但封装在IP数据报中：ICMP 报文作为 IP 层数据报的数据，加上数据报的首部，组成 IP 数据报发送出去。

ICMP 报文的格式



ICMP 报文类型

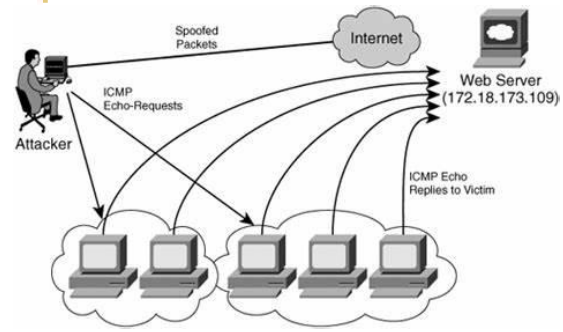
- 差错报告报文
  - 终点不可达：网络、主机、协议、端口不可达；需要分片但DF置1；源路由失败等
  - 源站抑制：拥塞指示
  - 超时：收到TTL为零的分组；在预定时间内不能收到全部分片，丢弃并发报告
  - 参数问题
  - 改变路由（重定向）
- 查询报文。
  - 回送请求和应答报文
  - 时间戳请求和应答报文
  - 掩码地址请求和应答报文
  - 路由器询问和通告报文

ICMP攻击

- 洪泛攻击（FLOOD ATTACK）
  - 向目的主机发送大量无用数据包，使目的主机忙于处理这些数据包，而无法提供正常服务的网络行为
- ICMP洪泛攻击
  - 对目的主机发送大量ping包，使得目的主机忙于处理ping包而无能力处理其他正常请求，被这些网络流量淹没，并开始丢弃合法的连接
    - Ping：Echo request/Echo reply
- Smurf攻击

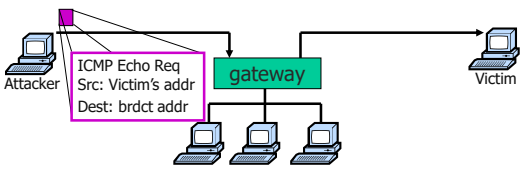
Smurf攻击

- 也称为放大攻击（amplifier attack）
- 攻击方法
  - 将ICMP数据包的源地址设置为目标的IP地址（第三方的受害者），并将目的地址设置为广播地址，发送经过修改的ICMP数据包
  - ICMP应答请求(ping)数据包淹没受害主机，最终由于该网络的所有主机都对此ICMP应答请求做出答复，导致网络阻塞。
  - 最终导致第三方崩溃。
- smurf放大器
  - 同一广播地址的一组主机的响应成为smurf放大器（smurf amplifier）



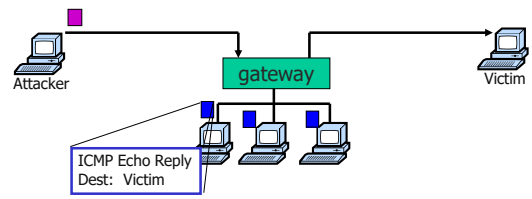
Smurf攻击过程

- 伪造源地址 (IP address, email account, ...)
- 重定向（Indirection）
  - 反射攻击Reflector attacks



Smurf攻击过程

- 伪造源地址 (IP address, email account, ...)
- 重定向（Indirection）
  - 反射攻击Reflector attacks



防御Smurf攻击

- 配置路由器禁止IP广播包进网
  - 例：在cisco路由器上配置如下：
    Router(config-if)# *no ip directed-broadcast*
- 配置网络上所有计算机的操作系统，禁止对目标地址为广播地址的ICMP包响应。
- 对于从本网络向外部网络发送的数据包，本网络应该将其源地址为其他网络的数据包过滤掉
- 2007年该漏洞得到了一定的修复，目前该攻击使用不多
  - ISP丢弃设置源路由选项的数据包
- 教训：不要使用放大器；避免反馈与回路
  - 例：IPv4的源路由选项（source routing）
  - IPv6修复该问题

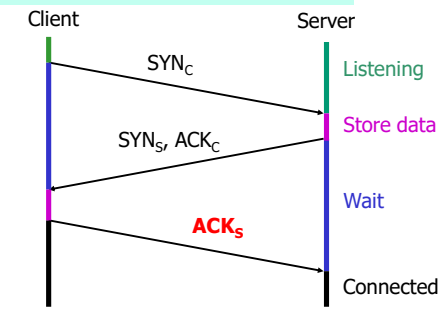
SYN洪泛攻击

SYN洪泛攻击（SYN Flood）

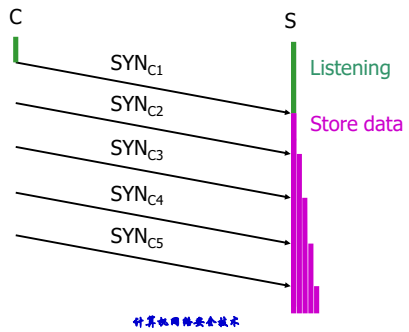
- SYN洪泛（SYN flood）攻击
  - 首次出现在1996年，
    CERT(Computer Emergency Response Team)不久就发布了对于这种攻击技术的初步评估与解决方案。
- SYN洪泛攻击的基础
  - TCP建立连接时三次握手
  - 第三个数据包验证连接发起人在第一次请求中使用的源IP地址上具有接收数据包的能力。
- 攻击方法
  - 试图发送足够多的SYN包，而不进行应答，导致接收方耗尽backlog队列。
  - 在此期间，服务器将不能响应其他应用程序合法的新TCP连接请求

SYN洪泛攻击（SYN Flood）

TCP正常建立连接的过程：三次握手

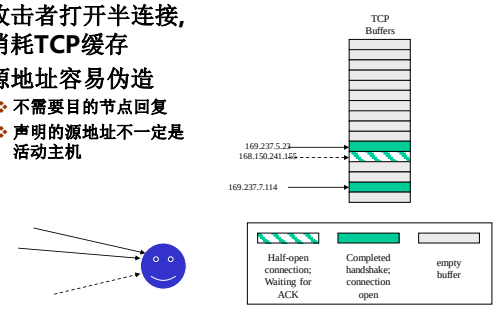


SYN洪泛攻击（SYN Flood）



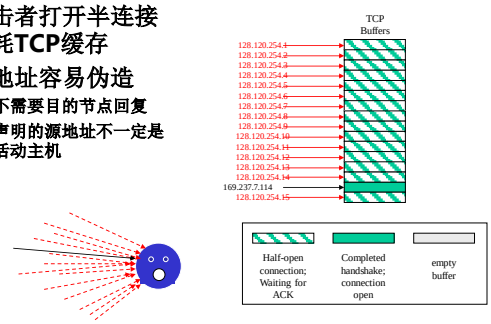
SYN洪泛攻击（SYN Flood）

- 攻击者打开半连接，消耗TCP缓存
- 源地址容易伪造
  - 不需要目的节点回复
  - 声明的源地址不一定是活动主机



SYN洪泛攻击（SYN Flood）

- 攻击者打开半连接 消耗TCP缓存
- 源地址容易伪造
  - 不需要目的节点回复
  - 声明的源地址不一定是活动主机

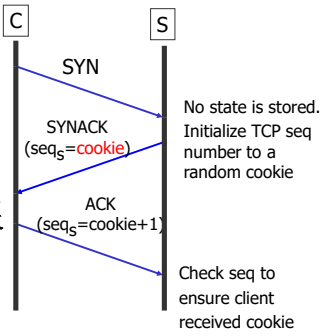


SYN洪泛攻击检测

- 攻击目标：连接内存（connection memory）→ 打开过多的半连接
  - 基于TCP的服务器，如Web server, FTP server, or mail server
- 检查SYN洪泛攻击（SYN Flood）
  - 运行 netstat -s |grep “listenqueue overflows”，检查连接状态
    - check whether many connections are in "SYN_RECEIVED"
- 如何防御?
  - 超时：服务器缩短半连接的超时时间（如20秒以下）
  - 使用SYN cookies 和 SYN caches 机制防止伪造IP攻击
    - SYN Cookie原理由D.J. Bernstain和Eric Schenk在1996年提出

SYN Cookie

- 目的：防止伪造源IP地址
- 在TCP服务器收到TCP SYN包并返回TCP SYN+ACK包时，不分配一个专门的数据区，而是根据这个SYN包计算出一个cookie值。
- 在收到TCP ACK包时，TCP服务器根据cookie值检查这个TCP ACK包的合法性。
- 如果合法，再分配专门的数据区进行处理未来的TCP连接



Linux内核中的SYN Cookie实现

- Linux内核中的SYN Cookie机制主要功能是防止本机遭受SYN Flood攻击。
  - Linux2.4.20内核：Linux内核对TCP流程的处理主要在tcp_ipv4.c文件中的函数实现
- 当处理TCP SYN包时，系统进入tcp_v4_conn_request函数。其中调用cookie_v4_init_sequence生成一个 ISN（Initial Sequence Number）。Linux内核把它作为SYN Cookie流程中的cookie。

cookie的计算

- cookie的计算应该包含本次连接的状态信息，使攻击者不能伪造。
- cookie的计算：
  - 服务器收到一个SYN包，计算一个消息摘要mac。
  - mac = MAC(A, k);
  - MAC是消息认证码函数，它能够提供cookie计算中需要的安全性。
    - 在Linux实现中，MAC函数为SHA1
  - A = SOURCE_IP || SOURCE_PORT || DST_IP || DST_PORT || t || MSSIND
  - k为服务器的密钥，实际上是一组随机数。
  - t为系统启动时间，每60秒加1
  - MSSIND为MSS对应的索引

验证cookie

- 把ACK包的ack_seq - 1，得到原来计算的cookie。把ACK包的seq - 1，得到SYN段的seq。
  - t1为服务器发送SYN Cookie的时间，单位为分钟，保留高12位
  - t2为收到ACK的时间，t2 - t1 < 4分钟，才是合法的。即ACK必须在4分钟内到达才行。
  - 验证mssind
- 如果t1和mssind都是合法的，则认为此ACK是合法的，可以直接完成三次握手。
- 时间戳对SYN Cookie非常重要
  - 如果不支持时间戳选项，则通过SYN Cookie建立的连接就会不支持大多数TCP选项。
- 只有在服务器的accept_queue满载时才会开启syn-cookie
  - 很耗时并且违背TCP端到端原则

SYN Cookie的特点

- SYN Cookie技术的有效性
  - 在建立连接的过程中不需要在服务器端保存任何信息，实现了无状态的三次握手，防止SYN洪泛攻击
- 存在问题
  - 由于cookie的计算只涉及到包头部分信息，在建立连接的过程中不在服务器端保存任何信息，所以失去了协议的许多功能，比如超时重传。
  - 计算cookie有一定的运算量，增加了连接建立的延迟时间，因此，SYN Cookie技术不能作为高性能服务器的防御手段。通常采用动态资源分配机制，
  - 可能导致另一种拒绝服务攻击方式，攻击者发送大量的ACK报文，服务器忙于计算验证。
- SYN Cookie Firewall
  - 利用SYN Cookie的原理在内网和外网之间实现TCP三次握手过程的**代理（proxy）的机制**

恶意数据包型DoS攻击

- **恶意数据包型DoS攻击利用某些操作系统的TCP/IP协议栈或是其他一些网络应用服务的软件实现中存在漏洞，构造一些非法、恶意的数据包，由于开发时没有预计到会出现这些非法数据包，系统相应的响应也是随机的。因此，这类攻击会递归执行，导致许多系统崩溃、停止响应等**
  - **Land攻击**
  - **死亡之ping攻击**
  - **TearDrop－泪滴攻击**
  - **畸形消息攻击**

Land攻击

- Land攻击原理是利用某些TCP/IP协议栈的三次握手过程实现中存在缺陷，而进行DoS攻击的
- Land攻击是向目标主机发送一个特殊的SYN包
  - 包中的源地址和目的地址都是目标主机的地址。
  - 目标主机收到这样的连接请求时会向自己发送SYN/ACK数据包，结果导致目标主机向自己发回ACK数据包并创建一个连接。
  - 大量的这样数据包使目标主机建立了很多无效的连接，系统资源被耗尽

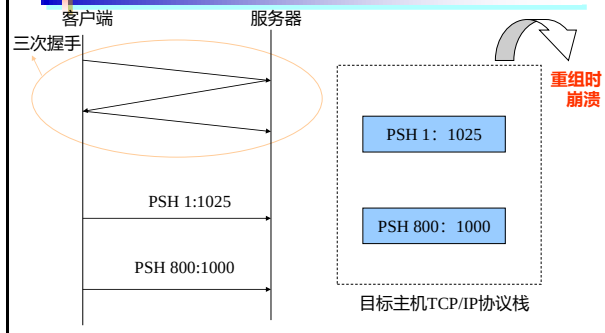
死亡之ping（Ping of Death）

- Ping程序使用的ICMP协议，而ICMP报文最大长度是固定的，64K
- 早期的很多操作系统在接收ICMP数据报文时，只开辟64K的缓冲区用于存放接收到的ICMP报文，并且没有检查接收到ICMP报文的实际长度
- ICMP报文的实际长度大于64K，则产生一个缓冲区溢出错误，导致TCP/IP协议堆栈崩溃。造成主机的重启动或死机
- 防御方法
  - 防火墙难以对这种攻击进行检测，因为每个分片包看起来都很正常
  - 对操作系统打补丁，使内核将不再对超过规定长度的包进行重组

泪滴（teardrop）攻击

- 泪滴(teardrop)攻击又称为分片攻击。它是一种典型的利用TCP/IP协议栈的漏洞进行DoS攻击
- Teardrop攻击主要是利用IP数据包的分片机制，通过发送重叠的分片偏移地址，使的TCP/IP协议栈无法正确的对IP分片重组，最终导致目标主机的TCP/IP协议栈的崩溃

Teardrop攻击示意图



畸形消息攻击

- 畸形消息攻击是一种有针对性的拒绝服务攻击方式，它利用操作系统或是应用程序存在某些处理消息时没有适当的错误校验的漏洞进行攻击。所以一旦收到这些畸形的消息，目标系统或程序就会崩溃
- 向IIS5服务器递交如下的URL会导致IIS5的停止服务

http://dstIP/…..[25kb of '.'] ….ida
GET /……..[3k]…….htr HTTP/1.0

其他资源消耗型的攻击

- SYN Flood
- ACK Flood
- ICMP Flood
- UDP Flood、UDP DNS Query Flood
- Connection Flood
- HTTP Get Flood

UDP FLOOD

- 常见的情况是利用大量UDP小包冲击DNS服务器或Radius认证服务器、流媒体视频服务器。
- 100k pps的UDPFlood经常造成线路上的骨干设备阻塞，造成整个网段的瘫痪。
- 在UDPFLOOD攻击中，攻击者可发送大量伪造源IP地址的小UDP包。
  - 由于UDP协议是无连接性的，所以只要开了一个UDP的端口提供相关服务的话，那么就可针对相关的服务进行攻击。

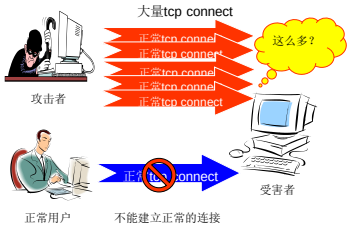
防御UDP FLOOD攻击

UDP协议是无连接状态的协议，并且UDP应用协议差异极大，因此针对UDP Flood的防护非常困难。

- 判断包大小，如果是大包攻击，则使用防止UDP碎片方法
  - 根据攻击包大小设定包碎片重组大小，通常不小于1500。在极端情况下，可以考虑丢弃所有UDP碎片。
- 攻击端口为业务端口：根据该业务UDP最大包长设置UDP最大包大小以过滤异常流量。
- 攻击端口为非业务端口：一个是丢弃所有UDP包，可能会误伤正常业务；一个是建立UDP连接规则，要求所有去往该端口的UDP包，必须首先与TCP端口建立TCP连接。不过这种方法需要专业防火墙或其他防护设备支持
- 资源消耗
  - UDP攻击是一种消耗对方资源，也消耗自己的资源的攻击方式

Connection Flood

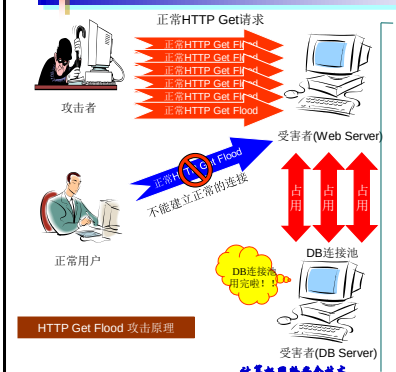
Connection Flood 攻击原理



攻击表象

- 利用真实 IP 地址（代理服务器、广告页面）在服务器上建立大量连接
- 服务器上残余连接(WAIT状态)过多，效率降低，甚至资源耗尽，无法响应
- 蠕虫传播过程中会出现大量源IP地址相同的包，对于 TCP 蠕虫则表现为大范围扫描行为
- 消耗骨干设备的资源，如防火墙的连接数

HTTP Get Flood



HTTP Get Flood 攻击原理

攻击表象

- 利用代理服务器向受害者发起大量HTTP Get请求
- 主要请求动态页面，涉及到数据库访问操作
- 数据库负载以及数据库连接池负载极高，无法响应正常请求

作业

- 举例说明Web服务器的三种安全漏洞
- 什么是拒绝服务攻击?
- ARP欺骗攻击的基本原理
- Smurf攻击的基本原理
- SYN flood攻击基本原理